

2
S. Bond
11/13/02
Attorney Docket No. 826.1787

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Kuniaki SHIMADA, et al.

Application No.:

Group Art Unit:

Filed: January 25, 2002

Examiner:

For: PACKET RELAY PROCESSING APPARATUS

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application Nos. 2001-090122 and 2001-308387

Filed: March 27, 2001 and October 4, 2001, respectively.

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 25, 2002

By: 

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

JC879 U.S. PTO
10/056091
01/28/02

JAPAN PATENT OFFICE



This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: March 27, 2001

Application Number: Patent Application
No. 2001-090122

Applicant(s): FUJITSU LIMITED

July 27, 2001

Commissioner,
Japan Patent Office Kozo OIKAWA

Certificate No. 2001-3065919

BEST AVAILABLE COPY

日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2001年 3月27日

出 願 番 号
Application Number:

特願2001-090122

出 願 人
Applicant(s):

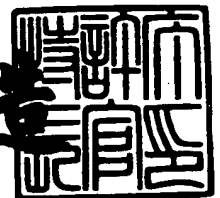
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 7月27日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3065919

【書類名】 特許願

【整理番号】 0150163

【提出日】 平成13年 3月27日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 13/00

【発明の名称】 パケット中継処理装置

【請求項の数】 10

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 嶋田 邦昭

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 横山 乾

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 栗田 敏彦

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 勝山 恒男

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 川崎 健

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

株式会社内

【氏名】 高場 浩一

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通
株式会社内

【氏名】 ▲蔭▼山 博靖

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100100930

【弁理士】

【氏名又は名称】 長澤 俊一郎

【電話番号】 03-3822-9271

【選任した代理人】

【識別番号】 100080894

【弁理士】

【氏名又は名称】 京谷 四郎

【電話番号】 03-3823-7935

【手数料の表示】

【予納台帳番号】 024143

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704945

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 パケット中継処理装置

【特許請求の範囲】

【請求項 1】 ネットワーク接続装置を有するパケット中継処理装置であって、

上記ネットワーク接続装置がセッション管理に基づくパケット中継処理部を備えている
ことを特徴とするパケット中継処理装置。

【請求項 2】 パケット中継処理装置のサーバが外部セッション管理機能を備え、

ネットワーク接続装置が、与えられた条件に応じてセッション情報を上記サーバに転送し、サーバによりセッション管理を行う
ことを特徴とする請求項 1 のパケット中継処理装置。

【請求項 3】 ネットワーク接続装置が処理振分部と複数のサービス処理部を備え、

上記処理振分部が、上記複数のサービス処理部へのパケットの振分を行いサービス処理を実行させる
ことを特徴とする請求項 1 のパケット中継処理装置。

【請求項 4】 パケット中継処理装置のサーバが外部サービス処理部を備え、

上記処理振分部が、与えられた条件によって、パケットを上記サーバに転送し、サーバの外部サービス処理部でサービス処理を実行させる
ことを特徴とする請求項 3 のパケット中継処理装置。

【請求項 5】 ネットワーク接続装置が処理振分部とサービス処理部を備え、また、パケット中継処理装置のサーバがパケット詳細解析部を備え、

上記処理振分部が、与えられた条件によってパケットをサーバに転送し、サーバがパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置に設定し、

ネットワーク接続装置は、以後同じセッションに対して上記決定されたサービ

ス内容に基づき中継処理を行う

ことを特徴とする請求項 1 のパケット中継処理装置。

【請求項 6】 パケット中継処理装置におけるネットワーク接続装置であって、

上記ネットワーク接続装置がセッション管理に基づくパケット中継処理部を備えている

ことを特徴とするネットワーク接続装置。

【請求項 7】 上記ネットワーク接続装置は処理振分部と複数のサービス処理部を備え、

上記処理振分部が、上記複数のサービス処理部へのパケットの振り分けを行い、サービス処理を実行させる

ことを特徴とする請求項 6 のネットワーク接続装置。

【請求項 8】 上記ネットワーク接続装置が処理振分部とサービス処理部を備え、

上記処理振分部が、与えられた条件によって、パケットをパケット中継処理装置のサーバに転送し、サーバでサービス内容を決定し、

ネットワーク接続装置のサービス処理部は、以後同じセッションに対して上記サーバで決定したサービス内容に基づき中継処理を行う

ことを特徴とする請求項 6 のネットワーク接続装置。

【請求項 9】 パケット中継装置のネットワーク接続装置で実行されるパケット中継処理プログラムであって、

上記パケット中継処理プログラムは、セッション管理に基づくパケット中継処理を行う

ことを特徴とするパケット中継処理装置におけるパケット中継処理プログラム。

【請求項 10】 ネットワーク接続装置を有するパケット中継処理装置のサーバで実行されるプログラムであって、

上記プログラムは、ネットワーク接続装置から転送されるパケットを解析して、サービス内容を決定し、該サービス内容をネットワーク接続装置に設定し、

ネットワーク接続装置は、以後、上記決定されたサービス内容に基づき、パケ

ットの中継処理を行う

ことを特徴とするパケット中継処理装置のサーバで実行されるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、サーバ負荷分散制御、NAT (Network Address Translation)、帯域制御、VPN (Virtual Private Network)、ファイアウォールサービス機能を持ったサーバを最適化するためのパケット中継処理装置に関する。

【0002】

【従来の技術】

現在、WWW (World Wide Web) や E-mail、携帯電話におけるパケット通信サービスの普及により、インターネットが急速に大規模化している。それに伴い、ネットワークのさらなる高速化や、セキュリティ等の高機能化の要求が高まって来ている。現状のネットワークサービスの実行形態は、サーバと、NIC (Network Interface Card) 等のネットワーク接続装置という構成が一般的である。昨今のネットワークサービスは複雑化してきており、様々な、そして新しい要求に対し柔軟に対応できるという点で、サーバというプラットフォームが適している。

【0003】

図24に従来のパケット中継処理装置の構成を示す。同図はサーバとネットワーク接続装置がネットワーク上で、サービスを実現する一般的な構成を示しており、矢印は制御情報の流れ、太い矢印はパケット情報を示す。

同図において、100はサーバであり、パケット処理部101と、サービス1処理部～サービスn処理部102と、サービス1制御部～サービスn制御部103を備える。

サービス1処理部～サービスn処理部102は、サービス1制御部～サービスn制御部103で定めるポリシーに従い、セッション管理やルーティングを行うとともに、フィルタリングや負荷分散等のサービス処理を行う。

104はネットワーク接続装置であり、ネットワーク接続部を介してネットワ

ークから入力されたパケットは、ネットワーク接続装置 1 0 4、パケット通信部 1 0 5 を介してサーバ 1 0 0 のパケット処理部 1 0 1 に送られ、パケットが処理される。

【0 0 0 4】

【発明が解決しようとする課題】

最近の急激なインターネットの大規模化のため、ネットワークを流れるパケットの量は指数関数的な伸びを示している。このため、従来のサーバでは、要求される処理速度に 대응できなくなっており、サーバを高速化する技術が求められている。また、新しいプラットフォームを作る上で、サーバの多くのサービスを統合することができるという点は、できる限り損なわないようにしたい。

本発明は上記問題を解決するためになされたものであって、多くのネットワークサービスで使用している共通処理を、ネットワーク接続装置に配置することにより、サーバのサービス処理を高速化することを目的とする。

【0 0 0 5】

【課題を解決するための手段】

図 1 は本発明の概要を説明する図である。同図において、1 はサーバ、2 はネットワーク接続装置であり、本発明においては、ネットワーク接続装置を統合し、従来サーバ上に配置していたパケット処理部とセッション管理部をネットワーク接続装置 2 上に配置してパケット中継処理部を構成し、該パケット中継処理部により、ネットワーク接続装置 2 上でセッション管理に基づくパケット中継処理を行う。

また、ネットワーク接続装置 2 上に、処理振分部 2 c と複数のサービス処理部 2 d を設け、サーバ 1 により設定されるポリシーに従って、処理振分部 2 c により、複数のサービス処理部 2 d へのセッション管理に基づく振り分けを行う。

さらに、サーバ 1 に外部セッション管理機能を設け、セッション数がネットワーク接続装置 2 のセッションテーブル登録数を上回った場合等に、サーバ 1 によりセッション管理を行うようにすることもできる。

また、サーバ 1 に外部サービス処理部を設け、上記処理振分部 2 c が、パケットを上記サーバ 1 に転送し、サーバ 1 の外部サービス処理部でサービス処理を実

行させるようにしたり、サーバ 1 にパケット詳細解析部を設け、サーバ 1 がパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置 2 に設定し、ネットワーク接続装置 2 は、以後同じセッションに対して上記決定されたサービス内容に基づき中継処理を行うようにすることもできる。

以上のように本発明においては、次のようにして前記課題を解決する。

(1) 上記ネットワーク接続装置 2 に、パケット処理部 2 a とセッション管理部 2 b からなる、セッション管理に基づくパケット中継処理部を設け、ネットワーク接続装置 2 により、セッション管理に基づく中継処理を行う。

上記のように、従来サーバ上に配置していた機能をネットワーク接続装置 2 で行っているため、サーバ 1 の CPU 使用率を下げるができる。また、ネットワーク接続装置 2 でセッション管理を行い、セッション開始時にセッションテーブルに出力先を登録しているため、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

(2) 上記 (1) において、パケット中継処理装置のサーバ 1 に外部セッション管理機能を設け、ネットワーク接続装置 2 が、与えられた条件に応じてセッション情報を上記サーバ 1 に転送し、サーバ 1 によりセッション管理を行う。

これにより、セッション数がネットワーク接続装置 2 のセッションテーブル登録数を上回った場合でも、ネットワーク接続装置 2 で溢れた分をサーバ 1 で管理することができる。

(3) 上記 (1) において、ネットワーク接続装置 2 に処理振分部 2 c と複数のサービス処理部 2 d を設け、処理振分部 2 c が、上記複数のサービス処理部 2 d へのパケットの振分を行いサービス処理を実行させる。

上記のように、処理振分部 2 c と複数のサービス処理部 2 d をサーバ 1 より高速に処理できるネットワーク接続装置 2 に配置することにより、サーバ 1 の CPU の使用率を小さくすることができるとともに、サービス処理を高速化することができる。

(4) 上記 (3) において、サーバ 1 に外部サービス処理部を設け、処理振分部 2 c が、与えられた条件によって、パケットの振分を行いサーバ 1 の外部サービス処理部でサービス処理を実行させる。

上記のようにサービス処理を、ネットワーク接続装置 2 とサーバ 1 の両方で実行できるようにすることにより、ネットワーク接続装置 2 上で実現するのは困難なサービス処理をサーバ 1 で行うことができ、ネットワークサービスが複雑な処理を必要とする場合でも対応することができる。

(5) 上記(1)において、ネットワーク接続装置 2 に処理振分部 2 c とサービス処理部 2 d を設け、また、サーバ 1 にパケット詳細解析部を設け、処理振分部 2 c が、与えられた条件によってパケットをサーバ 1 に転送し、サーバ 1 がパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置 2 に設定し、ネットワーク接続装置 2 は、以後同じセッションに対して上記決定されたサービス内容に基づき中継処理を行う。

上記のように、サーバ 1 においてパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置 2 に設定し、以後同じセッションに対してネットワーク接続装置 2 が上記決定されたサービス内容に基づき中継処理を行うようにすることにより、サーバ 1 で全ての処理を行う場合に比べ、サービス処理を高速に実現することが可能となる。

【0006】

【発明の実施の形態】

図 2 は本発明の第 1 の実施例のパケット中継処理装置の構成を示す図である。

同図において、11 はサーバであり、ネットワーク制御部 12 を備えており、ネットワーク制御部 12 は、管理者が入力したルーティング情報を制御情報通信部 31 を通して、ネットワーク接続装置 20 のルーティングテーブル 23 a に書き込む。制御情報通信部 31 は、例えば P C I バスやシリアルインターフェースである。

20 はネットワーク接続装置であり、本実施例のネットワーク接続装置 20 は、図 2 4 に示した複数のネットワーク接続装置 104 を統合したものであり、パケット処理部 21、セッション管理部 22、セッションテーブル 22 a、ルーティング処理部 23、ルーティングテーブル 23 a を備え、前記図 2 4 のサーバが行っていた、パケット処理、セッション管理、ルーティング処理等は、ネットワーク接続装置 20 で行われる。

図2において、ネットワークから入力された図3に示すパケットは、ネットワーク接続部30を通してネットワーク接続装置20のパケット処理部21に送られる。ネットワーク接続部30は、例えばイーサネットコントローラである。

パケット処理部21では、後述する図4のフローチャートに示す処理を行い、パケットをセッション管理部22に送る。セッション管理部22では、後述する図5のフローチャートに示すようにセッション管理を行い、パケットをパケット処理部21に渡す。

パケット処理部21は、後述する図4に示すようにパケットの処理を行い、パケットをネットワーク接続部30を介して、ネットワークに出力する。

【0007】

図4に上記パケット処理部の処理フローを示す。

同図に示すように、パケット処理部21では、ネットワークから入力されたパケットのバッファリングを行い、チェックサムのチェックを行う。ついで、デフラグメンテーションを行い、パケットをセッション管理部22へ送る。

そして、セッション管理部22から送られてくるパケットのフラグメンテーション、チェックサム再計算を行い、パケットをネットワークに出力する。なお、パケット処理部21における処理は従来のパケット処理部における処理と同じである。

【0008】

図5に上記セッション管理部22の処理フローを示す。

同図に示すように、セッション管理部22にパケットが送られてくると、セッション管理部22では、セッションテーブル22aを検索する。セッションテーブルは、セッションを管理するテーブルであり、図6に示すようにセッションを一意に決定するためのセッション識別子（宛先／送信元アドレス、宛先／送信元ポート、プロトコル）や、セッションの状態、および出力先などを持つ。

セッション管理部22は、パケットのIPヘッダ内の送信元／宛先IPアドレス、及びTCPヘッダ内のプロトコル、送信元／宛先ポートの情報をキーにして、セッションテーブルを検索する。

セッション管理部22に送られてきたパケットがセッションテーブル22aに

登録されていない場合には、セッションの最初の packets であるので、セッションテーブルに登録を行う。すなわち、図 6 に示すセッションテーブル 22a にセッション識別子（宛先／送信元アドレス、宛先／送信元ポート、プロトコル）や、セッションの状態を書き込む。

ついで、ルーティング処理部 23 でルーティングテーブル 23a の検索を行い、結果をセッションテーブル 22a に出力先を書き込む。

一方、セッションテーブルに登録がある場合には、セッションテーブル 22a のセッション状態を検査して、状態が遷移するかどうかを判定する。そして、状態が遷移する場合にはセッションテーブルの状態を書き換える。

そして、セッションの状態遷移が終わりセッションクローズの場合、すなわち状態が TIME_WAIT 及び CLOSED になっている場合には、セッションテーブルのエントリから削除する。そして、処理が終わった packets は出力先に送られる。

【0009】

上記状態遷移は、TCP とその他のプロトコルではその判断が異なる。以下、TCP とその他のプロトコルを分けて説明する。

図 7 に TCP の場合のセッション状態を示す。TCP の場合、セッション状態には図 7 に示すように、CLOSED、SYN_RECV、ESTAB、FIN_RECV、FIN_SENT、TIME_WAIT の 6 つの状態を設定する。

セッションテーブルのセッション状態には、図 6 に示すように CLOSED を除く上記 5 つの状態のうち、どの状態であるかが書き込まれている。

セッションが登録されていない時には状態が CLOSED になっており、この状態で SYN packets が到着した場合、SYN_RECV に状態遷移し、「セッション状態」を SYN_RECV に書き換える。ついで、ESTAB (Established) 状態に遷移し packets の送受信を行う。そして、FIN packets によりセッションは終了する。以下同様にして、SYN packets と FIN packets の到着を検知することにより、セッションの開始と終了を検知することができる。

【0010】

図 8 に T C P の場合のセッション開始からセッション終了までの状態遷移の様子の一例を示す。

同図に示すように、クライアントとサーバ間で通信を行う場合、まずクライアントから S Y N パケットを送信する。ついで、サーバから S Y N _ A C K パケットを返し、これに応答してクライアントからサーバに A C K パケットを送信する。これにより S Y N 状態から E S T A B (E s t a b l i s h e d) 状態に遷移し、以後、相互にパケットを送受信する。そして、セッションを終了する際、例えばクライアントから F I N パケットをサーバに送信し、サーバが F I N _ A C K を送信し、これに応答してクライアントから A C K を送信することによりセッションが終了する (C L O S E D 状態となる)。

これに対し、T C P 以外では、S Y N や F I N のフラグが存在しない。よって、図 9 に示すようにセッションに無いパケットが届いた場合には、状態を E S T A B とする。セッションの終了は検知することができないので、タイマーによって一定時間パケットの通過が無い場合にはセッションを削除することによって対応する。

【 0 0 1 1 】

以上説明したように、本実施例においては、ネットワーク接続装置にセッション管理に基づくパケット中継処理機能を設け、従来サーバ上に配置していた機能をネットワーク接続装置が果たすようにしたので、サーバの C P U の使用率を下げることができる。

また、ネットワーク接続装置にセッション管理部を設け、セッション開始時にセッションテーブルに出力先を登録しているので、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【 0 0 1 2 】

図 1 0 は本発明の第 2 の実施例のパケット中継処理装置の構成を示す図である。本実施例は、前記図 2 に示した第 1 の実施例のパケット中継処理装置において、セッション情報をサーバ 1 1 に転送するサーバ転送部 2 4、セッション情報の通信を行うセッション情報通信部 3 2、外部セッション管理部 1 3、外部セッシ

セッションテーブル13aを設けたものである。そして、ネットワーク接続装置20のセッションテーブルが一杯になったとき、サーバ11に設けた外部セッション管理部13によりセッション管理を行う。その他の動作は第1の実施例と同様である。

【0013】

図11に本実施例におけるセッション管理部、外部セッション管理部における処理フローを示す。

同図に示すように、セッション管理部22にパケットが送られてくると、セッション管理部22、外部セッション管理部13では、セッションテーブル22a、外部セッションテーブル13aを検索する。セッションテーブル22a、13aは前記図6で説明したセッションを管理するテーブルである。

セッション管理部22に送られてきたパケットがセッションテーブル22a及び外部セッションテーブル13aに登録されていない場合には、セッションの最初のパケットであるので、まずセッションテーブル22aが一杯かを調べる。

セッションテーブル22aが一杯でない場合には、前記したようにセッションテーブルに登録を行う。ついで、ルーティング処理部23でルーティングテーブル23aの検索を行い、結果をセッションテーブルに出力先を書き込む。

また、セッションテーブル22aに登録がある場合には、セッションテーブル22aのセッション状態を検査して、状態が遷移するかどうかを判定する。そして、状態が遷移する場合にはセッションテーブルの状態を書き換える。

そして、セッションの状態遷移が終わった後、セッションクローズの場合には、セッションテーブル22aのエントリから削除する。処理が終わったパケットは出力先に送られる。

【0014】

一方、セッションの最初のパケットを登録する際、セッションテーブル22aが一杯の場合には、サーバ11の外部セッション管理部13で上記と同様の処理を行う。

すなわち、前記したように外部セッションテーブル13aにパケットの登録を行い、ルーティングテーブルの検索を行って、結果を外部セッションテーブル1

3 a に出力先を書き込む。

また、外部セッションテーブル 1 3 a に登録がある場合には、外部セッションテーブル 1 3 a のセッション状態を検査して、状態が遷移するかどうかを判定する。状態が遷移する場合には外部セッションテーブル 1 3 a の状態を書き換える。そして、セッションの状態遷移が終わった後、セッションクローズの場合には、セッションテーブル 1 3 a のエントリから削除する。

【 0 0 1 5 】

以上のように、本実施例においては、ネットワーク接続装置にセッション管理に基づくパケット中継処理機能を設け、従来サーバ上に配置していた機能をネットワーク接続装置が果たすようにしたので、第 1 の実施例と同様、サーバの CPU の使用率を下げるができる。また、第 1 の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

さらに、セッション数がネットワーク接続装置のセッションテーブル登録数を上回った場合、サーバ 1 1 に設けた外部セッション管理部 1 3 でセッション管理を行っているので、ネットワーク接続装置で溢れた分をサーバ 1 1 で管理することができる。

一般に、ネットワーク接続装置は高速であるがメモリ等の制限がサーバよりきつい。そこで、上記のように構成すれば、セッション数がネットワーク接続装置のセッションテーブル登録数を上回った場合でも、セッション管理を行うことが可能となる。

なお、上記説明ではサーバ 1 1 に外部セッション管理部 1 3 を設けてサーバ 1 1 でセッション管理を行っているが、サーバ 1 1 に外部セッションテーブル 1 3 a のみを設け、セッション管理はネットワーク接続装置 2 0 のセッション管理部で行い、セッションテーブル 2 2 a で溢れたセッションを上記外部セッションテーブル 1 3 a に登録するようにしてもよい。

【 0 0 1 6 】

図 1 2 は本発明の第 3 の実施例のパケット中継処理装置の構成を示す図である。本実施例は、ネットワーク接続装置に処理振分部とサービス処理部とポリシー

テーブルを設け、サーバにより設定されるポリシーに従って、ネットワーク接続装置がフィルタリング、負荷分散、NAT等のサービス処理を実行する実施例を示している。

同図において、11はサーバであり、サーバ11はサービス制御部14を備えており、サービス制御部14は、制御情報通信部31を通して、ネットワーク接続装置20のポリシーテーブル25にポリシーを書き込む。ここで、ポリシーとは、フィルタリング等のサービスを実行するためのルールである。例えば、フィルタリングの場合には、ポリシー識別子の範囲で廃棄か通過かを設定する。負荷分散の場合には、仮想（代表）IPアドレス、ポート番号と、振分先全てのサーバのIPアドレス、ポート番号を設定する。NATの場合には、変換後IPアドレス、ポート番号を設定する。

20はネットワーク接続装置であり、本実施例のネットワーク接続装置20は、第1の実施例と同様、パケット処理部21、セッション管理部22、セッションテーブル22a'を備えるとともに、上記ポリシーテーブル25、パケットに対する適用サービスを判別し各サービスに必要な処理を行う処理振分部26、複数のサービス処理部27を備えている。

【0017】

図12において、ネットワークから入力されたパケットは、ネットワーク接続部30を通り、パケット処理部21に送られる。

パケット処理部21は、前記した図4の処理フローに示したように、入力したパケットのバッファリングとチェックサムチェック、デフラグメンテーションを行い、セッション管理部22へ送る。そして、セッション管理部22から送られてきたパケットに対して、フラグメントとチェックサム再計算を行い、ネットワーク接続装置30を介して、ネットワークに出力する。

【0018】

本実施例のセッション管理部22の処理フローを図13に示す。

同図に示すように、パケットがセッション管理部22に送られてくると、まず図14に示すセッションテーブル22a'を検索する。

セッションテーブル22a'は、前記したようにセッションを管理するテーブ

ルであり、セッションを一意に決定するためのセッション識別子（宛先/送信元アドレスおよびポート、プロトコル）や、セッションの状態、および出力先が登録され、さらに本実施例においては適用サービスタイプ（フィルタリングや負荷分散など）、そのサービス固有の情報（振り分け先アドレスなど）等を持つ。

セッションテーブルの検索は、第1の実施例と同様、パケットのIPヘッダ内の送信元/宛先IPアドレス、及びTCPヘッダ内のプロトコル、送信元/宛先ポートの情報をキーにする。

セッションテーブル22a'の登録が無い場合、セッションの最初のパケットであるので、そのセッションに対する適用サービスを判定するため、図15に示すポリシーテーブル25の検索を行う。

【0019】

ポリシーテーブル25は、ルーティング情報を持つとともに、サービスを適用する範囲を指定するポリシー識別子（宛先/送信元アドレスおよびポート、プロトコル。任意や範囲指定でもよい）や適用サービス（フィルタリング廃棄や負荷分散など）、そのサービス固有の情報（全ての振り分け先アドレスなど）、および、優先度を持つ。

ポリシーテーブルとセッションがマッチした場合、そのポリシーをセッションテーブル22a'の適用サービスタイプの欄に書き込む。ただし、複数のポリシーにマッチした場合には、ポリシーテーブル25の優先度が高い順に処理する。また、同一サービスが複数マッチした場合には、優先度が最も高いものを採用し、残りは無効とする。

セッションテーブル22a'のセッション状態遷移に関しては、第1の実施例で説明したのと同様である。すなわち、セッションテーブルに登録がある場合には、セッションテーブル22a'のセッション状態を検査して、状態が遷移するかどうかを判定する。そして、状態が遷移する場合にはセッションテーブルの状態を書き換える。そして、セッションの状態遷移が終わった後、セッションテーブルのエントリから削除する。処理が終わったパケットは、処理振分部26に送られる。

【0020】

処理振分部 2 6 / サービス処理部 2 7 の処理フローを図 1 6 に示す。

処理振分部 2 6 / サービス処理部 2 7 では、パケットに対して適用サービスを判別し、各サービスに必要な処理を行う。

図 1 6 において、入力パケットに対応するセッションテーブル 2 2 a' に、ルーティング先が書き込まれていない場合、ポリシーテーブル 2 5 のルーティングテーブルを引き、出力先インターフェースと宛先 M A C アドレスをセッションテーブル 2 2 a' に書き込む。

また、セッションテーブル 2 2 a' の適用サービスタイプを参照し、入力パケットが、負荷分散サービスを実行するパケットであり、振分先がまだ決定していない場合、振分先サーバを決定し、対応するセッションテーブル 2 2 a' のサービス固有情報欄に書き込む。入力パケットがフィルタリング廃棄サービスを実行するパケットならば、パケットを廃棄する。

そして、入力パケットが、負荷分散もしくは N A T サービスを実行するパケットならば、パケットの I P ヘッダと T C P ヘッダ上の送信元 / 宛先 I P アドレス、送信元 / 宛先ポート等を、セッションテーブル 2 2 a' に従って書き換える。

以上のように、本実施例においては、第 1 の実施例と同様、サーバの C P U の使用率を下げることができ、また、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

さらに、処理振分部と複数のサービス処理部をサーバより高速に処理できるネットワーク接続装置に配置したので、サーバの C P U の使用率を小さくすることができるとともに、サービス処理を高速化することができる。

【 0 0 2 1 】

図 1 7 は本発明の第 4 の実施例のパケット中継処理装置の構成を示す図である。本実施例は、上記第 3 の実施例のパケット中継処理装置において、処理振分部 2 6 にサーバ転送機能を設けるとともに、サーバ 1 1 に外部サービス処理部 1 5 を設け、サービス処理を、ネットワーク接続装置とサーバの両方で実行できるようにしたものである。本実施例において、サービス処理をサーバで実行する場合には、ポリシーテーブル 2 5 にサービスの内容だけでなく、サーバに転送することを設定しておく。その他の動作は第 3 の実施例と同様である。

本実施例の処理振分部 2 6 / サービス処理部 2 7 の処理フローを図 1 8 に示す。図 1 8 において、ヘッダ書換処理までの処理は図 1 6 と同じであり、入力パケットに対応するセッションテーブル 2 2 a' に、ルーティング先が書き込まれていない場合、ポリシーテーブル 2 5 のルーティングテーブルを引き、出力先インターフェースと宛先 M A C アドレスをセッションテーブル 2 2 a' に書き込む。

また、セッションテーブル 2 2 a' の適用サービスタイプを参照し、適用サービスタイプにサーバ転送が設定されていない場合には、前記図 1 6 で説明したように、適用サービスタイプに応じた処理を行い、ヘッダ書換えパケットの場合、ヘッダの書換処理を行う。

ついで、サーバ転送該当パケットかを判断する。ポリシーテーブル 2 5 の適用サービスタイプにサーバ転送が設定されている場合には、パケット通信部 3 3 を介してパケットをサーバ 1 1 の外部サービス処理部 1 5 に転送する。

【 0 0 2 2 】

外部サービス処理部 1 5 の処理フローは前記した図 1 6、上記図 1 8 と同様であり、ルーティング先が未決定の場合、ルーティング先を決定し、出力先インターフェースと宛先 M A C アドレスをセッションテーブル 2 2 a' に書き込む。

また、入力パケットが、負荷分散サービスを実行するパケットであり、振分先がまだ決定していない場合、振分先サーバを決定し、対応するセッションテーブル 2 2 a' のサービス固有情報欄に書き込む。入力パケットがフィルタリング廃棄サービスを実行するパケットならば、パケットを廃棄する。

そして、入力パケットが、負荷分散もしくは N A T サービスを実行するパケットならば、パケットの I P ヘッダと T C P ヘッダ上の送信元 / 宛先 I P アドレス、送信元 / 宛先ポート等を、セッションテーブル 2 2 a' に従って書き換える。

【 0 0 2 3 】

なお、以上では、外部サービス処理部が、ネットワーク接続装置におけるサービス内容と同じサービスを行う場合について説明したが、外部サービス処理部で、例えば、暗号化、復号化、プロキシ、コンテンツ変換、プロトコル変換等のネットワーク接続装置上で行わないサービス処理を行うようにしてもよい。

以上のように本実施例においては、ネットワーク接続装置にセッション管理に

基づくパケット中継処理機能を設け、従来サーバ上に配置していた機能をネットワーク接続装置が果たすようにしたので、第 1 の実施例と同様、サーバの CPU の使用率を下げる事ができる。また、第 1 の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。さらに、処理振分部 2 6 にサーバ転送機能を設けるとともに、サーバ 1 1 に外部サービス処理部 1 5 を設け、サービス処理を、ネットワーク接続装置とサーバの両方で実行できるようにしたので、ネットワーク接続装置上で実現するのは困難なサービス処理をサーバで行うことができ、ネットワークサービスが複雑な処理を必要とする場合でも対応することができる。

【 0 0 2 4 】

図 1 9 は本発明の第 5 の実施例のパケット中継処理装置の構成を示す図である。本実施例は、サーバにパケット詳細解析部を設け、ネットワーク接続装置の処理振分部が、与えられた条件によってパケットをサーバに転送し、サーバがパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置に設定し、以後同じセッションに対してネットワーク接続装置が上記決定されたサービス内容に基づき中継処理を行うようにしたものである。

図 1 9 において、1 1 はサーバであり、サーバ 1 1 は前記第 3、第 4 の実施例と同様、サービス制御部 1 4 を備えており、サービス制御部 1 4 は、前記したように制御情報通信部 3 1 を通して、ネットワーク接続装置 2 0 のポリシーテーブル 2 5 にポリシーを書き込む。また、サーバ 1 1 はパケット詳細解析部 1 6 を備えており、パケット詳細解析部 1 6 は、パケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置のセッションテーブルに設定する。これにより、以後、ネットワーク接続装置 2 0 は上記サービス内容に基づき中継処理を行う。

【 0 0 2 5 】

2 0 はネットワーク接続装置であり、本実施例のネットワーク接続装置 2 0 は、第 3 の実施例と同様、パケット処理部 2 1、セッション管理部 2 2、セッションテーブル 2 2 a'、ポリシーテーブル 2 5、処理振分部 2 6、サービス処理部 2 7 を備えており、さらに処理振分部 2 7 はパケットのサーバ転送機能を備えて

いる。

上記パケット処理部 2 1、セッション管理部 2 2、処理振分部 2 6、サービス処理部 2 7 の動作は前記第 3 の実施例と同様であり、セッションテーブル 2 2 a、ポリシーテーブル 2 5 も前記図 1 4、図 1 5 に示した構成を備えている。

また、本実施例においては、予めサーバ 1 1 によりポリシーテーブルの適用サービスの欄に、上記パケット詳細解析部 1 6 に転送するパケットと適用サービスの適用範囲（例えば h t t p は U R L フィルタリング適用対象のパケットである等）を設定し、処理振分部 2 7 は、前記第 4 の実施例で説明したのと同様に、ポリシーテーブルを参照してサーバ 1 1 に転送するパケットを判断し、該当パケットを、ヘッダに適用サービスの種類を付してパケット通信路 3 3 を介してサーバ 1 1 のパケット詳細解析部 1 6 に転送する。

図 2 0 は処理振分部／サービス処理部の処理フローを示す図であり、ヘッダ書換処理までの処理は図 1 8 と同じであり、ヘッダ書換処理後、サーバ転送該当パケットかを判断し、ポリシーテーブル 2 5 の適用サービスタイプにサーバ転送が設定されている場合には、パケット通信部 3 3 を介してパケットをサーバ 1 1 のパケット詳細解析部 1 6 に転送する。

【 0 0 2 6 】

図 2 1 は、パケット詳細解析部 1 6 の処理フローを示す図であり、本実施例においては、U R L フィルタリング、U R L 負荷分散サービスをパケット詳細解析部 1 6 を用いて提供する場合について説明する。

まず、U R L フィルタリングサービスについて説明する。

予めサーバ 1 1 のサービス制御部 1 4 が、「パケット詳細解析部 1 6 へパケットを転送し U R L フィルタリングを行う」というポリシーを、制御通信情報部を介してポリシーテーブル 2 5 に設定する。

設定された条件から、ネットワーク接続装置 2 0 の処理振分部 2 6 が該当パケットをパケット詳細解析部 1 6 に転送する。

【 0 0 2 7 】

パケット詳細解析部 1 6 では、セッション状態を管理し、受信パケットをそのままネットワークへ出力させる。セッション状態が E S T A B となった後、図 2

1に示すように、HTTPのGETリクエストを受信したら、URLを判定し、通過／廃棄を決定する。すなわち、予め設定されたURLのリストを参照して、URLの通過／廃棄を判定し、廃棄の場合には、パケットを廃棄し、セッションテーブル22a'の適用サービスタイプの欄を、「サーバ転送・URLフィルタリング」から「廃棄」に書き換える。また、通過の場合には、適用サービスタイプの欄を「通過」に書き換える。

上記のように、パケット詳細解析部16が、ネットワーク接続装置20のセッションテーブルの適用サービスを、サーバ転送から通過／廃棄に設定し直すと、ネットワーク接続装置20は上記通過条件に従い、以後のパケットを処理する。すなわち、サーバのパケット詳細解析部16にパケットを転送することなく、パケットを通過させたり、廃棄する。

【0028】

図22は、上記URLフィルタリングの動作を説明する図である。

クライアント、サーバ間で、SYN、SYN__ACK、ACKパケットを交換しESTABの状態に遷移するまでは、上記パケット詳細解析部16にパケットが転送され、「ネットワーク接続装置20」+「サーバ11」で処理が行われる。

ESTAB状態に遷移し、HTTPのGETリクエスト（GET" http://www.xxx.co.jp"のようにURLが付されている）を受信すると、パケット詳細解析部16は、リストを参照して上記URLのパケットが廃棄するパケットであるか通過させるパケットであるかを判定し、セッションテーブルの適用サービス欄を廃棄または通過に書き換える。

以後、ネットワーク接続装置20は、セッションテーブルに設定された適用サービスに応じて、セッションが終了するまで、パケットを廃棄または通過させる。

【0029】

次に、URL負荷分散サービスについて説明する。

URL負荷分散は、まずサーバ11のサービス制御部14が、「パケット詳細解析部へサーバ転送しURL負荷分散を行う」というポリシーを、制御通信情報

部 3 1 を介してポリシーテーブル 2 5 の適用サービス欄に設定する。

設定された条件から、ネットワーク接続装置 2 0 の処理振分部 2 6 が該当パケットをサーバ 1 1 のパケット詳細解析部 1 6 に転送する。

パケット詳細解析部 1 6 では、クライアントとの間にコネクションを確立する。セッション状態が E S T A B となった後、H T T P の G E T リクエストを受信したら、U R L を判定し、予め設定された U R L のリストを参照して、振分先サーバを決定する。

その後、振分先サーバとコネクションを確立し、I P アドレス、ポート番号の書き換え、およびシーケンス番号／A C K 番号の書き換えをネットワーク接続装置のセッションテーブルに設定することにより、2 つのコネクションを1 つのコネクションとして扱う。そして、サーバに H T T P の G E T リクエストを送出する。

以後のパケットは、パケット詳細解析部 1 6 は送られず、ネットワーク接続装置 2 0 内で I P アドレス、ポート番号、シーケンス番号、A C K 番号を書き換えネットワークに出力される。

【 0 0 3 0 】

図 2 3 は、上記 U R L 負荷分散サービスの動作を説明する図である。

クライアント、パケット中継処理装置間で S Y N、S Y N _ A C K、A C K パケットを交換する。E S T A B 状態に遷移し、H T T P の G E T リクエストを受信すると、パケット詳細解析部 1 6 は、G E T リクエストの U R L を判定し、振分先サーバを決定する。

ついで、上記と同様に、パケット中継処理装置と振分先サーバの間で S Y N、S Y N _ A C K、A C K パケットを交換し、振分先サーバに H T T P の G E T リクエストを送出する。ここまでは、「ネットワーク接続装置 2 0」＋「サーバ 1 1」で処理が行われる。

以後、セッションが終了するまで、ネットワーク接続装置 2 0 が、セッションテーブルの設定に応じて、クライアントと振分先サーバとの間の中継処理を行う。

【 0 0 3 1 】

以上のように、本実施例においては、ネットワーク接続装置にセッション管理に基づくパケット中継処理機能を設け、従来サーバ上に配置していた機能をネットワーク接続装置が果たすようにしたので、第 1 の実施例と同様、サーバの CPU の使用率を下げるができる。また、第 1 の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

さらに、サーバのパケット詳細解析部においてパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置に設定し、以後同じセッションに対してネットワーク接続装置が上記決定されたサービス内容に基づき中継処理を行うようにしたので、サーバで全ての処理を行う場合に比べ、サービス処理を高速に実現することができる。

【 0 0 3 2 】

(付記 1) ネットワーク接続装置を有するパケット中継処理装置であって、

上記ネットワーク接続装置がセッション管理に基づくパケット中継処理部を備えている

ことを特徴とするパケット中継処理装置。

(付記 2) パケット中継処理装置のサーバが外部セッション管理機能を備え、

ネットワーク接続装置が、与えられた条件に応じてセッション情報を上記サーバに転送し、サーバによりセッション管理を行う

ことを特徴とする付記 1 のパケット中継処理装置。

(付記 3) ネットワーク接続装置が処理振分部と複数のサービス処理部を備え、

上記処理振分部が、上記複数のサービス処理部へのパケットの振分を行いサービス処理を実行させる

ことを特徴とする付記 1 のパケット中継処理装置。

(付記 4) パケット中継処理装置のサーバが外部サービス処理部を備え、

上記処理振分部が、与えられた条件によって、パケットを上記サーバに転送し、サーバの外部サービス処理部でサービス処理を実行させる

ことを特徴とする付記 3 のパケット中継処理装置。

(付記 5) ネットワーク接続装置が処理振分部とサービス処理部を備え、また

、パケット中継処理装置のサーバがパケット詳細解析部を備え、

上記処理振分部が、与えられた条件によってパケットをサーバに転送し、サーバがパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置に設定し、

ネットワーク接続装置は、以後同じセッションに対して上記決定されたサービス内容に基づき中継処理を行う

ことを特徴とする付記 1 のパケット中継処理装置。

(付記 6) パケット中継処理装置におけるネットワーク接続装置であって、

上記ネットワーク接続装置がセッション管理に基づくパケット中継処理部を備えている

ことを特徴とするネットワーク接続装置。

(付記 7) ネットワーク接続装置が、与えられた条件に応じてセッション情報をパケット中継装置のサーバに転送するサーバ転送部を備え、サーバは転送されたセッション情報によりセッション管理を行う

ことを特徴とする付記 6 のネットワーク接続装置。

(付記 8) 上記ネットワーク接続装置は処理振分部と複数のサービス処理部を備え、

上記処理振分部が、上記複数のサービス処理部へのパケットの振り分けを行い、サービス処理を実行させる

ことを特徴とする付記 6 のネットワーク接続装置。

(付記 9) 上記処理振分部が、与えられた条件によって、パケットをパケット中継装置のサーバに転送し、サーバにサービス処理を実行させる

ことを特徴とする付記 8 のネットワーク接続装置。

(付記 10) 上記ネットワーク接続装置が処理振分部とサービス処理部を備え、

上記処理振分部が、与えられた条件によって、パケットをパケット中継処理装置のサーバに転送し、サーバでサービス内容を決定し、

ネットワーク接続装置のサービス処理部は、以後同じセッションに対して上記サーバで決定したサービス内容に基づき中継処理を行う

ことを特徴とする付記 6 のネットワーク接続装置。

(付記 1 1) パケット中継装置のネットワーク接続装置で実行されるパケット中継処理プログラムであって、

上記パケット中継処理プログラムは、セッション管理に基づくパケット中継処理を行うことを特徴とするパケット中継処理装置におけるパケット中継処理プログラム。

(付記 1 2) 上記中継処理プログラムは、サーバ転送プログラムを備え、

上記サーバ転送プログラムは、与えられた条件に応じてセッション情報をパケット中継装置のサーバに転送し、サーバによりセッション管理を実行させることを特徴とする付記 1 1 のパケット中継処理装置におけるパケット中継処理プログラム。

(付記 1 3) 上記中継処理プログラムは、処理振分プログラムを備え、

上記処理振分プログラムは、ネットワーク接続装置の複数のサービス処理部へのパケットの振り分けを行い、サービス処理を実行させることを特徴とする付記 1 1 のパケット中継処理装置におけるパケット中継処理プログラム。

(付記 1 4) 上記処理振分プログラムは、与えられた条件によって、サーバへパケットを転送し、サーバにサービス処理を実行させることを特徴とする付記 1 3 のパケット中継処理装置におけるパケット中継処理プログラム。

(付記 1 5) 上記パケット中継処理プログラムは、処理振分プログラムを備え、

処理振分プログラムは、与えられた条件によって中継処理装置のサーバへパケットを転送し、

上記パケット中継処理プログラムは、以後、上記サーバで決定されたサービス内容に基づきパケットの中継処理を行うことを特徴とする付記 1 1 のパケット中継処理プログラム。

(付記 1 6) ネットワーク接続装置を有するパケット中継処理装置のサーバで実行されるプログラムであって、

上記プログラムは、サービス処理に関するポリシーを決定してネットワーク接続装置に設定し、

ネットワーク接続装置は、上記ポリシーに従って、サービス処理を行うことを特徴とするパケット中継処理装置のサーバで実行されるプログラム。

(付記 1 7) ネットワーク接続装置を有するパケット中継処理装置のサーバで実行されるプログラムであって、

上記プログラムは、サービス処理プログラムを備え、該プログラムにより、ネットワーク接続装置から転送されるパケットに対してサービス処理を行うことを特徴とする付記 1 6 のパケット中継処理装置のサーバで実行されるプログラム。

(付記 1 8) ネットワーク接続装置を有するパケット中継処理装置のサーバで実行されるプログラムであって、

上記プログラムは、ネットワーク接続装置から転送されるパケットを解析して、サービス内容を決定し、該サービス内容をネットワーク接続装置に設定し、

ネットワーク接続装置は、以後、上記決定されたサービス内容に基づき、パケットの中継処理を行うことを特徴とするパケット中継処理装置のサーバで実行されるプログラム。

(付記 1 9) パケット中継装置のネットワーク接続装置で実行されるパケット中継処理プログラムを記録した記録媒体であって、

上記パケット中継処理プログラムは、セッション管理に基づくパケット中継処理を行うことを特徴とするパケット中継処理装置におけるパケット中継処理プログラムを記録した記録媒体。

(付記 2 0) 上記中継処理プログラムは、サーバ転送プログラムを備え、

上記サーバ転送プログラムは、与えられた条件に応じてセッション情報をパケット中継装置のサーバに転送し、サーバによりセッション管理を実行させることを特徴とする付記 1 7 のパケット中継処理装置におけるパケット中継処理プログラムを記録した記録媒体。

(付記 2 1) 上記中継処理プログラムは、処理振分プログラムを備え、 上記

処理振分プログラムは、ネットワーク接続装置の複数のサービス処理部へのパケットの振り分けを行い、サービス処理を実行させることを特徴とする付記 1 7 のパケット中継処理装置におけるパケット中継処理プログラムを記録した記録媒体。

(付記 2 2) 上記処理振分プログラムは、与えられた条件によって、サーバへパケットを転送し、サーバにサービス処理を実行させることを特徴とする付記 1 9 のパケット中継処理装置におけるパケット中継処理プログラムを記録した記録媒体。

(付記 2 3) パケット中継処理プログラムは、処理振分プログラムを備え、
処理振分プログラムは、与えられた条件によって中継処理装置のサーバへパケットを転送し、

上記パケット中継処理プログラムは、以後、上記サーバで決定されたサービス内容に基づきパケットの中継処理を行う

ことを特徴とする付記 1 9 のパケット中継処理プログラムを記録した記録媒体。

(付記 2 4) ネットワーク接続装置を有するパケット中継処理装置のサーバで実行されるプログラムを記録した記録媒体であって、

上記プログラムは、サービス処理に関するポリシーを決定してネットワーク接続装置に設定し、

ネットワーク接続装置は、上記ポリシーに従って、サービス処理を行うことを特徴とするパケット中継処理装置のサーバで実行されるプログラムを記録した記録媒体。

(付記 2 5) ネットワーク接続装置を有するパケット中継処理装置のサーバで実行されるプログラムを記録した記録媒体であって、

上記プログラムは、サービス処理プログラムを備え、該プログラムにより、ネットワーク接続装置から転送されるパケットに対してサービス処理を行う

ことを特徴とする付記 2 4 のパケット中継処理装置のサーバで実行されるプログラムを記録した記録媒体。

(付記 2 6) ネットワーク接続装置を有するパケット中継処理装置のサーバで実行されるプログラムを記録した記録媒体であって、

上記プログラムは、ネットワーク接続装置から転送されるパケットを解析して、サービス内容を決定し、該サービス内容をネットワーク接続装置に設定し、

ネットワーク接続装置は、以後、上記決定されたサービス内容に基づき、パケットの中継処理を行う

ことを特徴とするパケット中継処理装置のサーバで実行されるプログラムを記録した記録媒体。

【 0 0 3 3 】

【発明の効果】

以上説明したように、本発明においては、以下の効果を得ることができる。

(1) 上記ネットワーク接続装置にセッション管理に基づくパケット中継処理部を設け、ネットワーク接続装置により、セッション管理に基づく中継処理を行うようにしたので、サーバのCPU使用率を下げることができる。また、ネットワーク接続装置上でセッション管理を行い、セッション開始時にセッションテーブルに出力先を登録することにより、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

(2) パケット中継処理装置のサーバに外部セッション管理機能を設け、ネットワーク接続装置からセッション情報を上記サーバに転送し、サーバによりセッション管理を行うことにより、セッション数がネットワーク接続装置のセッションテーブル登録数を上回った場合でも、ネットワーク接続装置で溢れた分をサーバで管理することができる。

(3) 処理振分部と複数のサービス処理部をサーバに比べ高速に処理できるネットワーク接続装置に配置することにより、サーバのCPUの使用率を小さくすることができるとともに、サービス処理を高速化することができる。

(4) サーバに外部サービス処理部を設け、サービス処理を、ネットワーク接続装置とサーバの両方で実行できるようにすることにより、ネットワーク接続装置2上で実現するのは困難なサービス処理をサーバで行うことができ、ネットワークサービスが複雑な処理を必要とする場合でも対応することができる。

(5) サーバにおいてパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置に設定し、以後同じセッションに対してネットワー

ク接続装置が上記決定されたサービス内容に基づき中継処理を行うようにすることにより、サーバで全ての処理を行う場合に比べ、サービス処理を高速に実現することが可能となる。

【図面の簡単な説明】

【図 1】

本発明の概要を説明する図である。

【図 2】

本発明の第 1 の実施例のパケット中継処理装置の構成を示す図である。

【図 3】

転送パケットのフレーム構成を示す図である。

【図 4】

パケット処理部の処理フローを示す図である。

【図 5】

セッション管理部の処理フローを示す図である。

【図 6】

セッションテーブルの構成例を示す図である。

【図 7】

T C P の状態遷移を示す図である。

【図 8】

T C P のセッション開始からセッション終了までの状態遷移を説明する図である。

【図 9】

U D P の状態遷移を示す図である。

【図 1 0】

本発明の第 2 の実施例のパケット中継処理装置の構成を示す図である。

【図 1 1】

第 2 の実施例のセッション管理部、外部セッション管理部における処理フローを示す図である。

【図 1 2】

本発明の第 3 の実施例のパケット中継処理装置の構成を示す図である。

【図 1 3】

本発明の第 3 の実施例のセッション管理部の処理フローを示す図である。

【図 1 4】

セッションテーブルの構成例を示す図である。

【図 1 5】

ポリシーテーブルの構成例を示す図である。

【図 1 6】

第 3 の実施例の処理振分部／サービス処理部の処理フローを示す図である。

【図 1 7】

本発明の第 4 の実施例のパケット中継処理装置の構成を示す図である。

【図 1 8】

第 4 の実施例の処理振分部／サービス処理部の処理フローを示す図である。

【図 1 9】

本発明の第 5 の実施例のパケット中継処理装置の構成を示す図である。

【図 2 0】

第 5 の実施例の処理振分部／サービス処理部の処理フローを示す図である。

【図 2 1】

パケット詳細解析部の処理フローを示す図である。

【図 2 2】

URL フィルタリングの動作を説明する図である。

【図 2 3】

URL 負荷分散サービスの動作を説明する図である。

【図 2 4】

従来のパケット中継処理装置の構成を示す図である。

【符号の説明】

- 1 サーバ
- 2 ネットワーク接続装置
- 1 1 サーバ

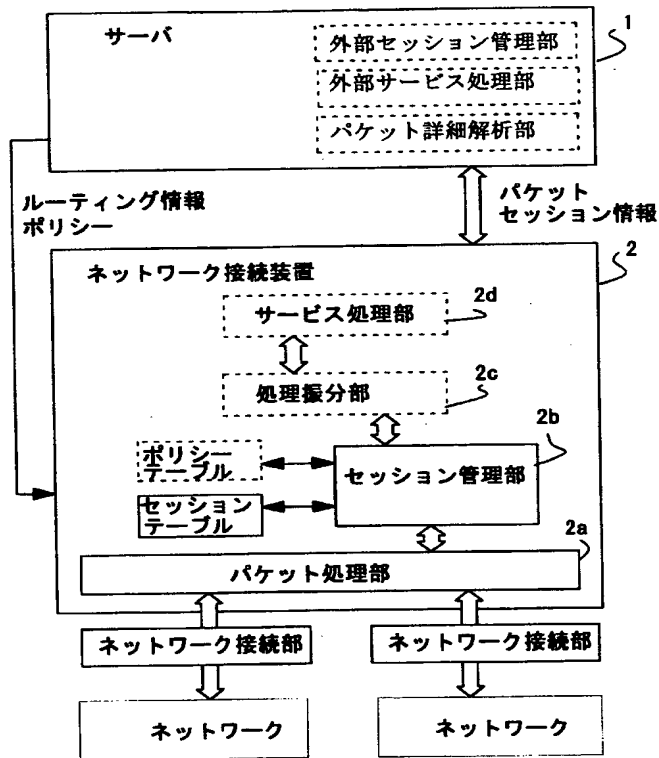
- 1 2 ネットワーク制御部
- 1 3 外部セッション管理部
- 1 3 a 外部セッションテーブル
- 1 4 サービス制御部
- 1 5 外部サービス処理部
- 1 6 パケット詳細解析部
- 2 0 ネットワーク接続装置
- 2 1 パケット処理部
- 2 2 セッション管理部
- 2 2 a セッションテーブル
- 2 2 a' セッションテーブル
- 2 3 ルーティング処理部
- 2 3 a ルーティングテーブル
- 2 4 サーバ転送部
- 2 5 ポリシーテーブル
- 2 6 処理振分部
- 2 7 サービス処理部
- 3 0 ネットワーク接続部
- 3 1 制御情報通信部
- 3 2 セッション情報通信部
- 3 3 パケット通信路

【書類名】

図面

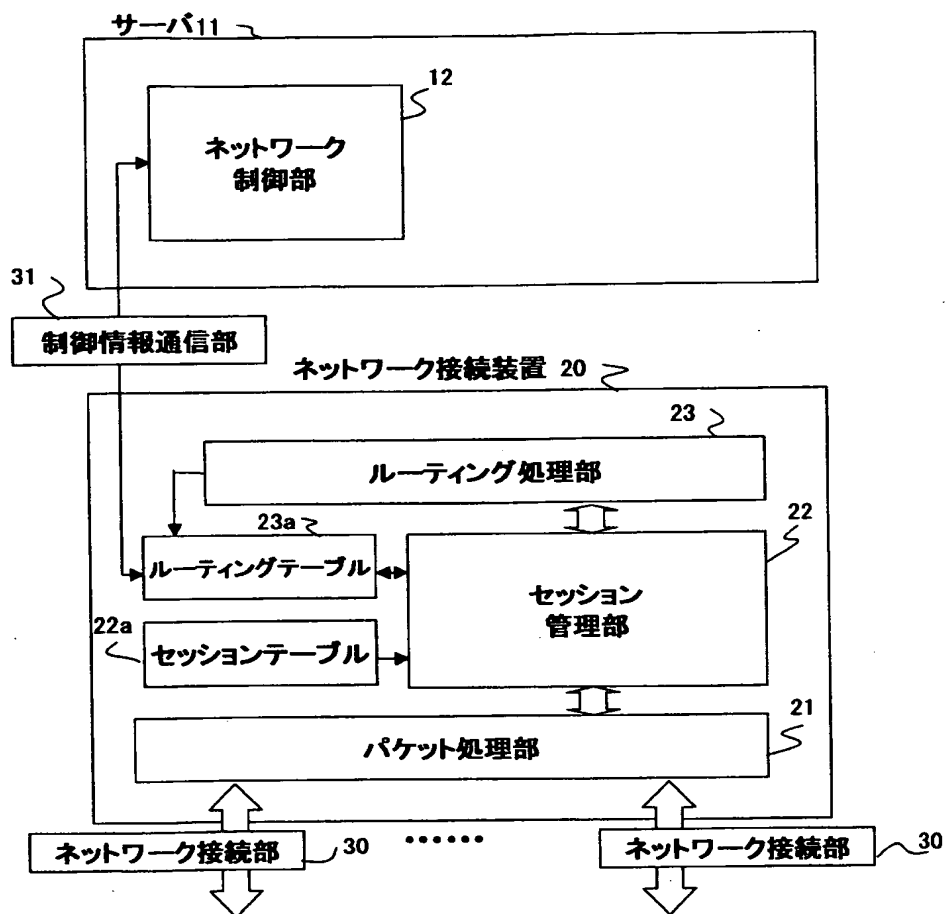
【図 1】

本発明の概要を示す図



【図 2】

本発明の第1の実施例のパケット中継処理装置の構成を示す図



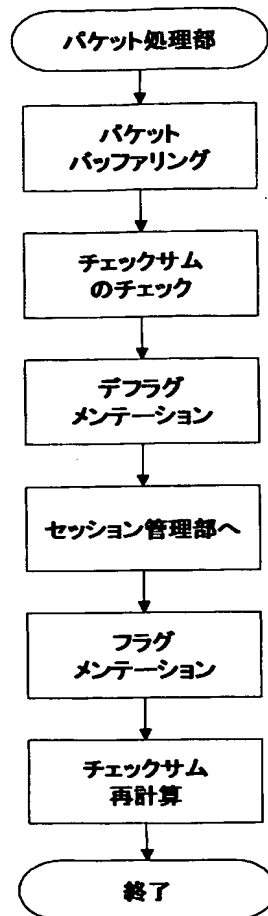
【図 3】

転送パケットのフレーム構成を示す図

イーサネット ヘッダ	IPヘッダ	TCP/UDP ヘッダ	データ
---------------	-------	----------------	-----

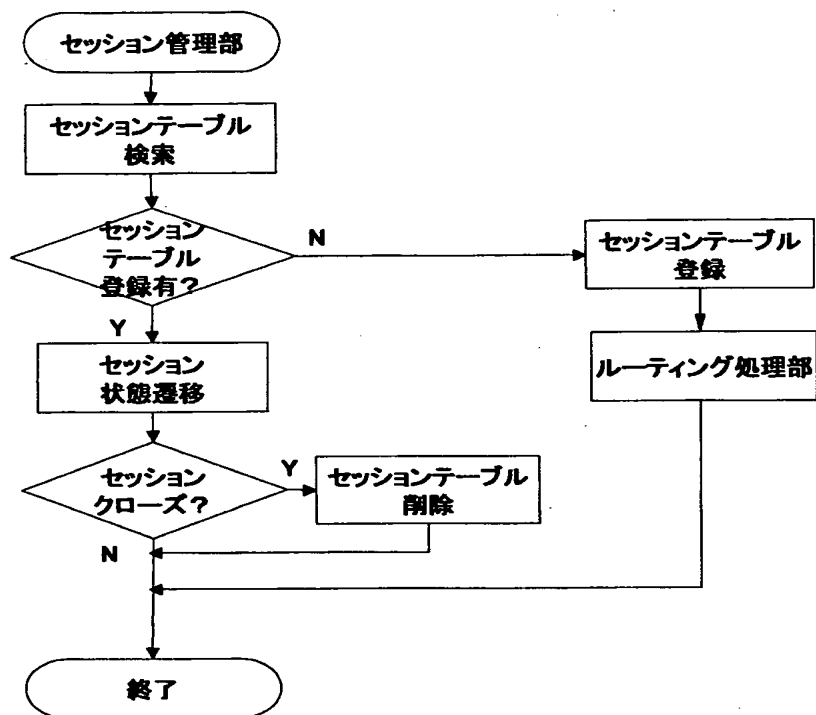
【図 4】

パケット処理部の処理フローを示す図



【図 5】

セッション管理部の処理フローを示す図



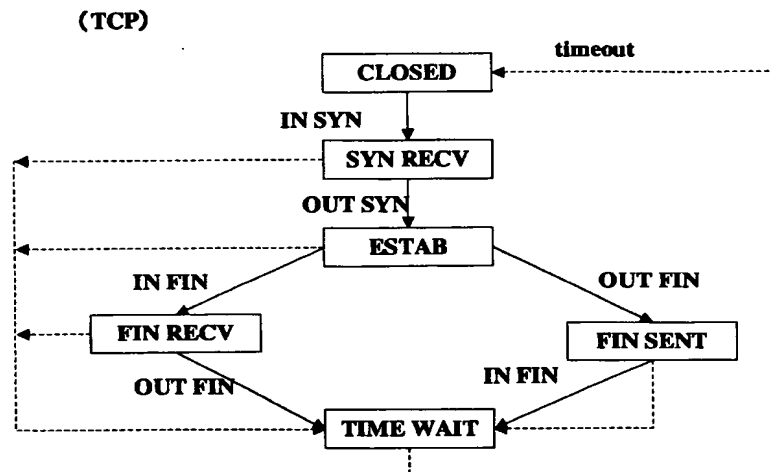
【図 6】

セッションテーブルの構成例を示す図

セッション識別子						
送信元IPアドレス	送信元ポート	プロトコル	宛先IPアドレス	宛先ポート	セッション状態	出力先
192.168.100.14	13200	TCP	192.168.10.5	8080	ESTAB	
192.168.10.5	8080	TCP	192.168.100.14	13200	ESTAB	
192.168.100.100	http	TCP	10.25.1.230	9250	IN SYN	
10.25.1.230	9250	TCP	192.168.100.75	http	IN SYN	

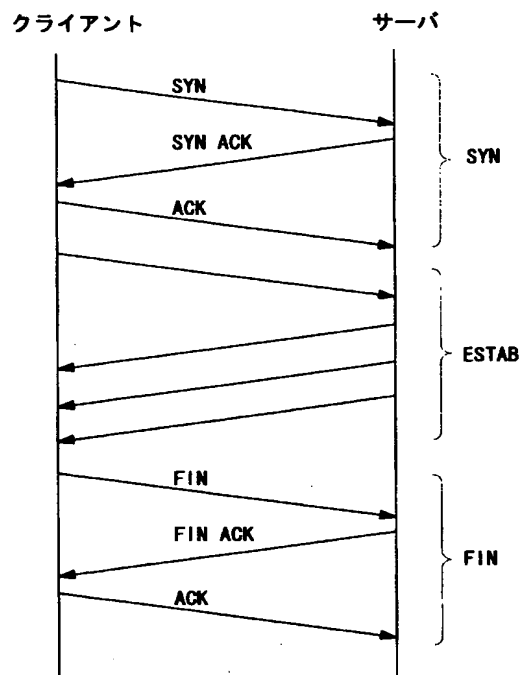
【図 7】

T C P の状態遷移を示す図



【図 8】

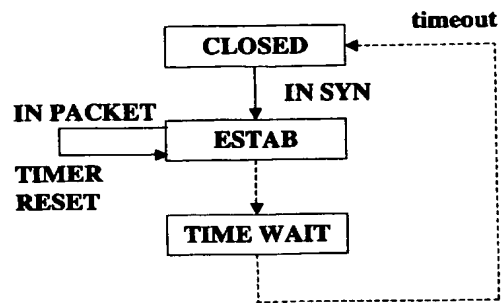
T C P のセッション開始から終了までの状態遷移を説明する図



【図 9】

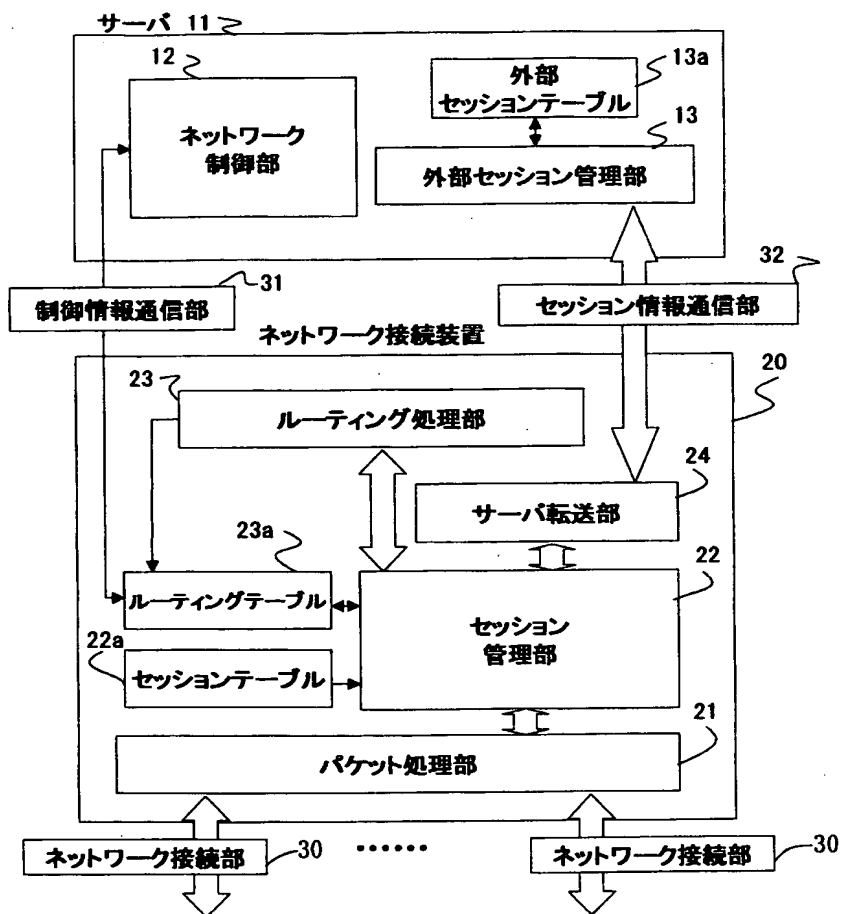
UDP の状態遷移を示す図

(UDP)



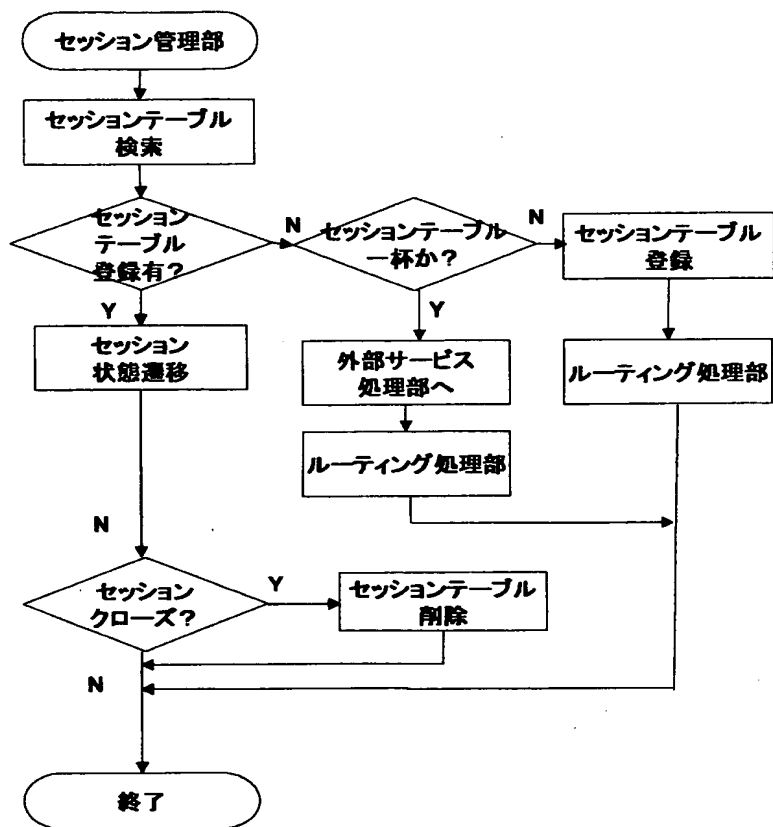
【図 10】

本発明の第2の実施例のパケット中継処理装置の構成を示す図



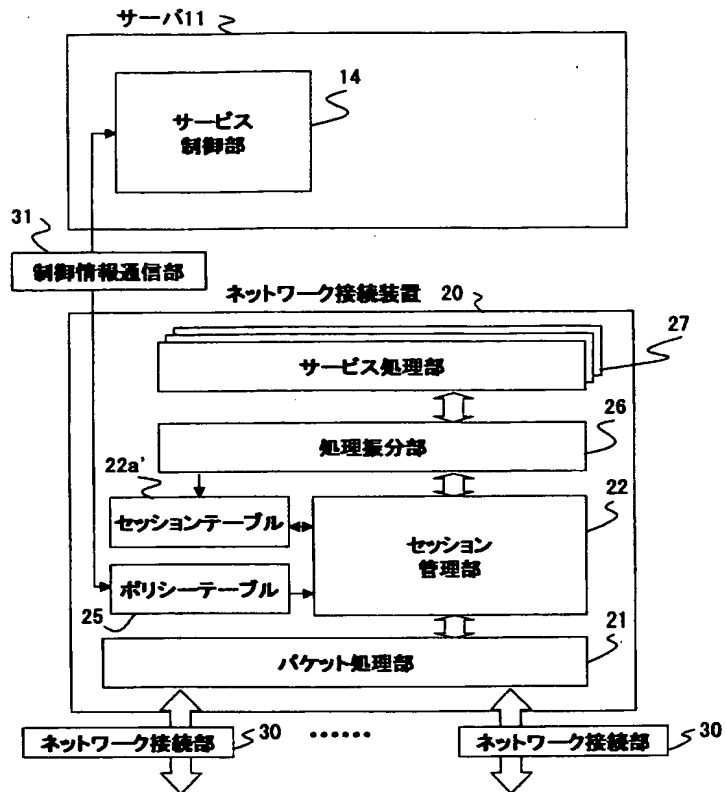
【図 1 1】

第 2 の実施例のセッション管理部、外部セッション管理部における
処理フローを示す図



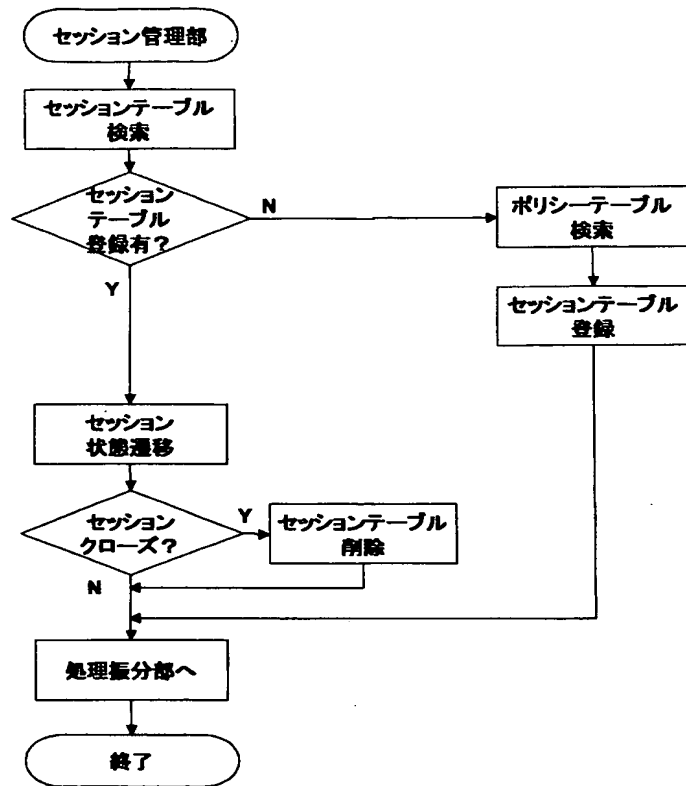
【図 1 2】

本発明の第 3 の実施例のパケット中継処理装置の構成を示す図



【図 1 3】

本発明の第 3 の実施例のセッション管理部の処理フローを示す図



【図 1 4】

セッションテーブルの構成例を示す図

セッション識別子						セッション状態	適用サービスタイプ	固有情報	出力先
送信元IPアドレス	送信元ポート	プロトコル	宛先IPアドレス	宛先ポート	宛先ポート				
192.168.100.14	13200	TCP	192.168.10.5	8080	8080	ESTAB	フィルタリング通過		
192.168.10.5	8080	TCP	192.168.100.14	13200	13200	ESTAB	フィルタリング通過		
192.168.100.100	http	TCP	10.25.1.230	9250	9250	IN SYN	NAT	192.168.100.75	
10.25.1.230	9250	TCP	192.168.100.75	http	http	IN SYN	負荷分散	192.168.100.100	

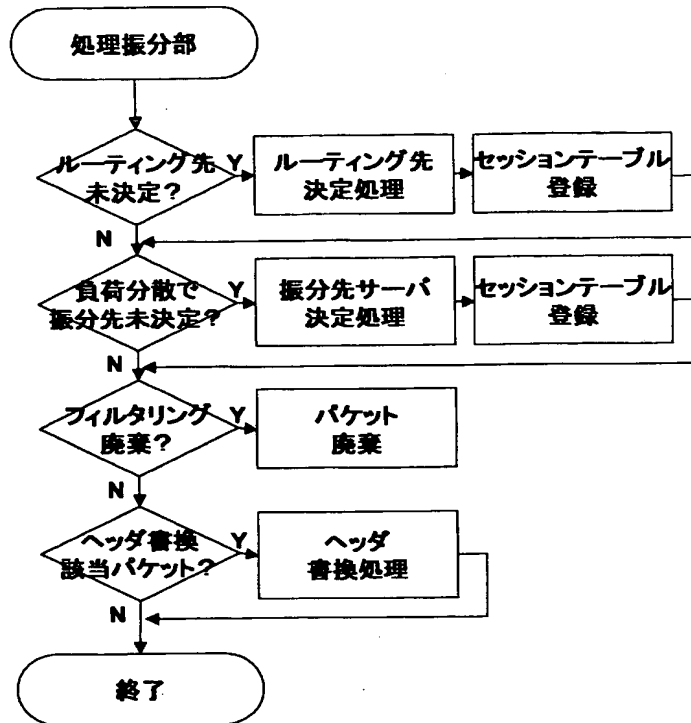
【図 1 5】

ポリシーテーブルの構成例を示す図

ポリシー識別子							
送信元IPアドレス	送信元ポート	プロトコル	宛先IPアドレス	宛先ポート	適用サービス	サービス固有情報	優先度
Any	Any	Any	Gw	Any	フィルタリング 廃棄		1000
Any	Any	TCP	仮想IPアドレス	http	負荷分散	振り分け先1, 2, 3, 4	5000

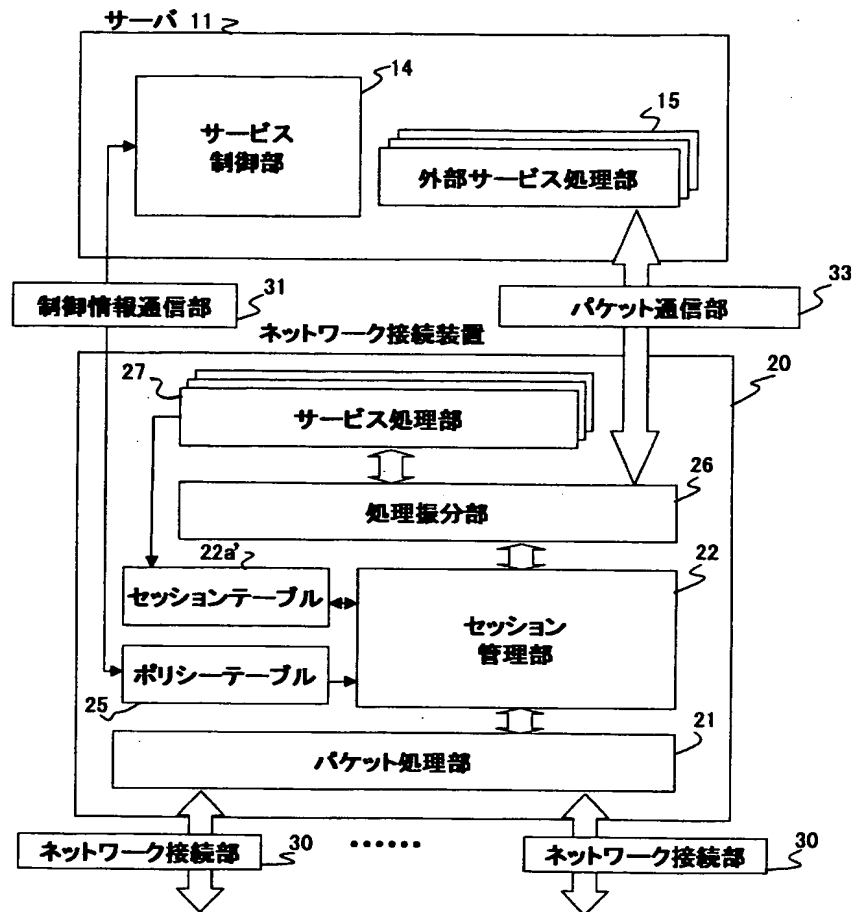
【図 1 6】

第 3 の実施例の処理振分部／サービス処理部の処理フローを示す図



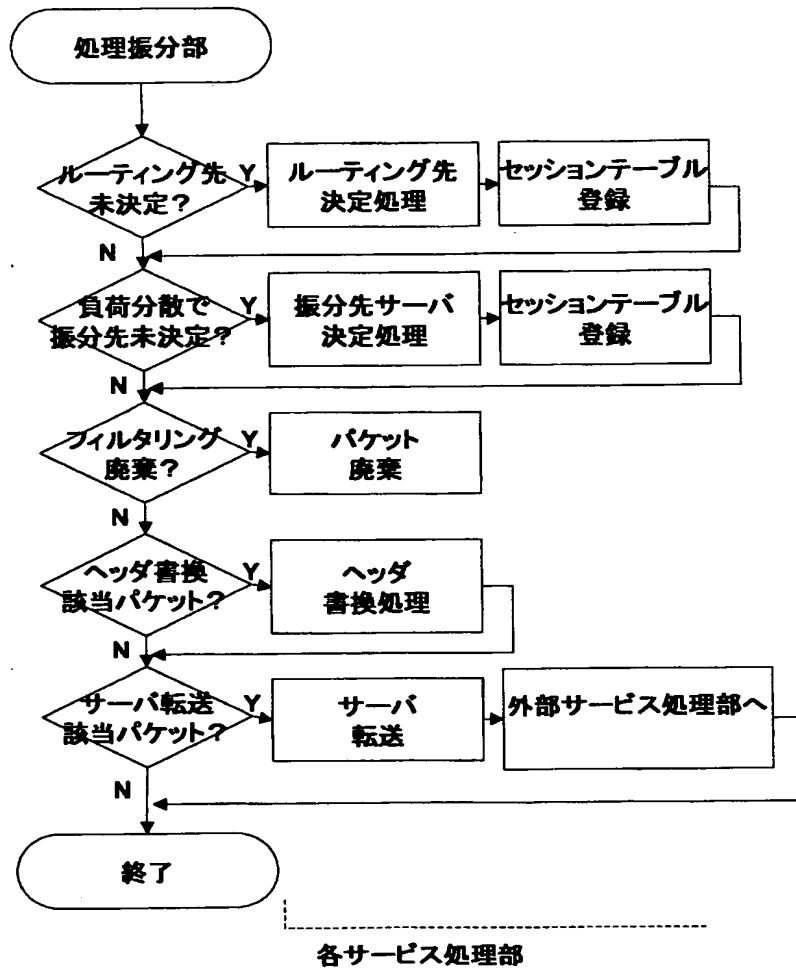
【図 17】

本発明の第4の実施例のパケット中継処理装置の構成を示す図



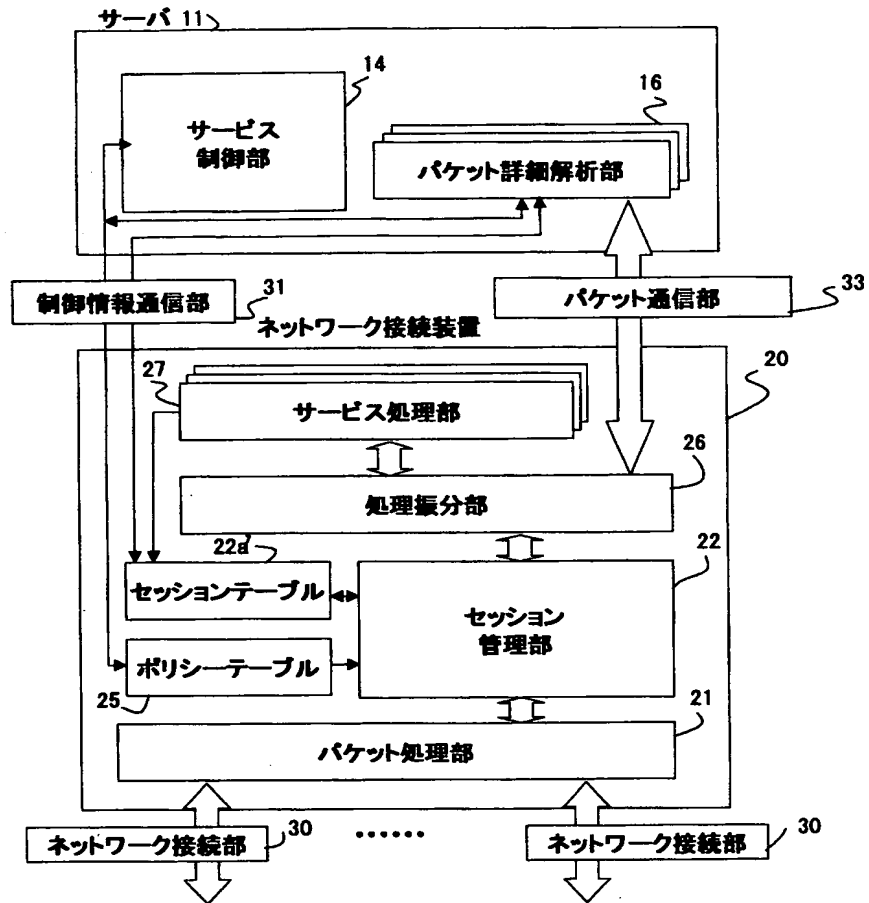
【図 1 8】

第 4 の実施例の処理振分部／サービス処理部の処理フローを示す図



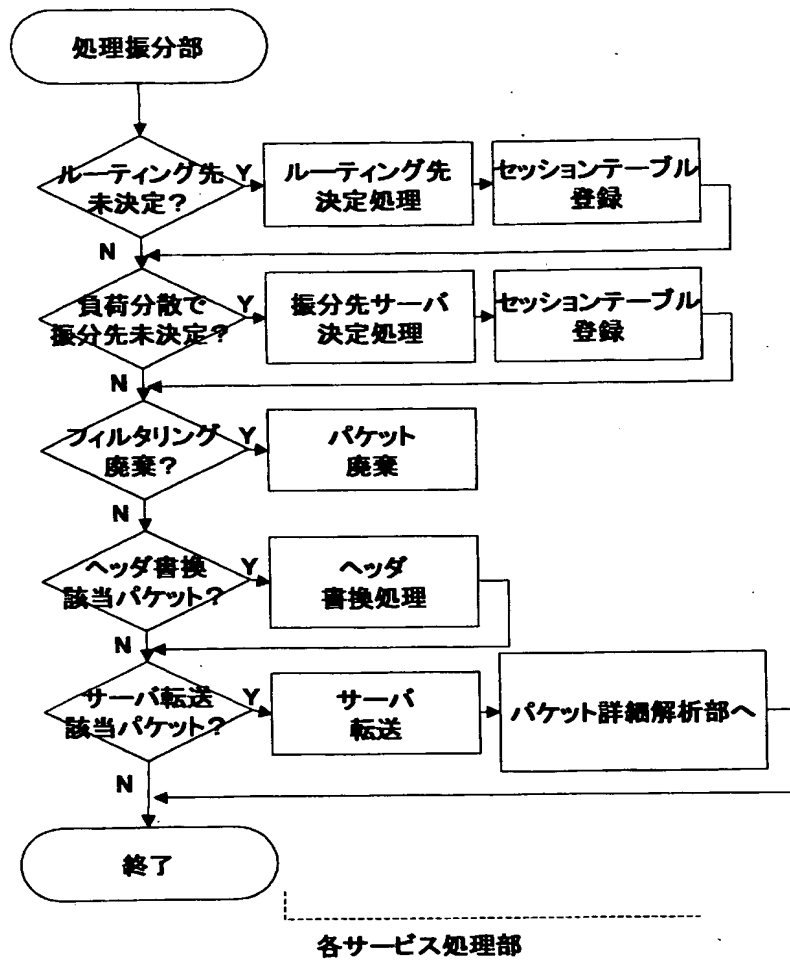
【図 19】

本発明の第5の実施例の packets 中継処理装置の構成を示す図



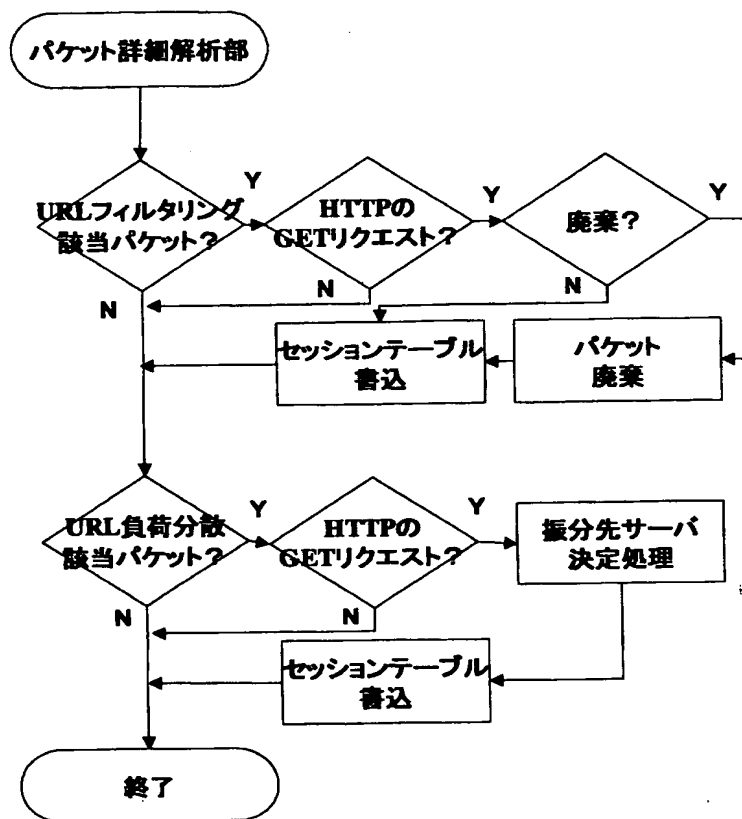
【図 2 0】

第 5 の実施例の処理振分部／サービス処理部の処理フローを示す図



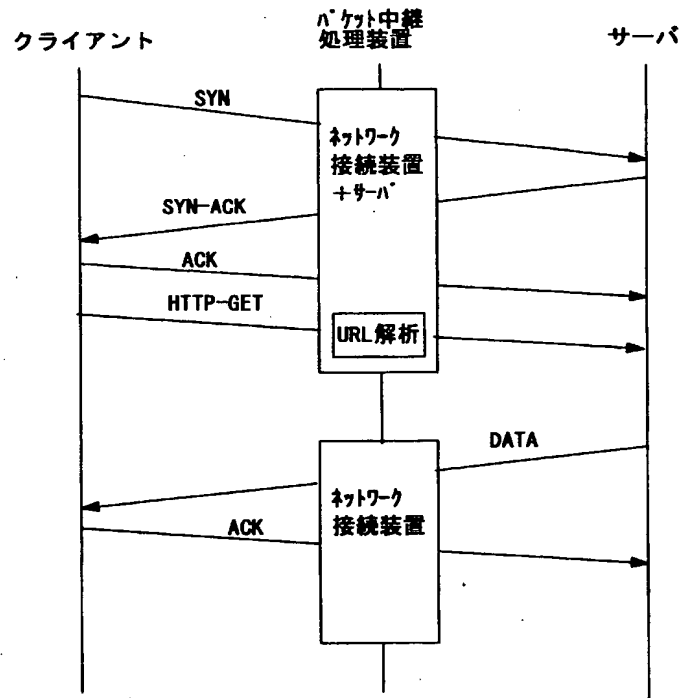
【図 21】

パケット詳細解析部の処理フローを示す図



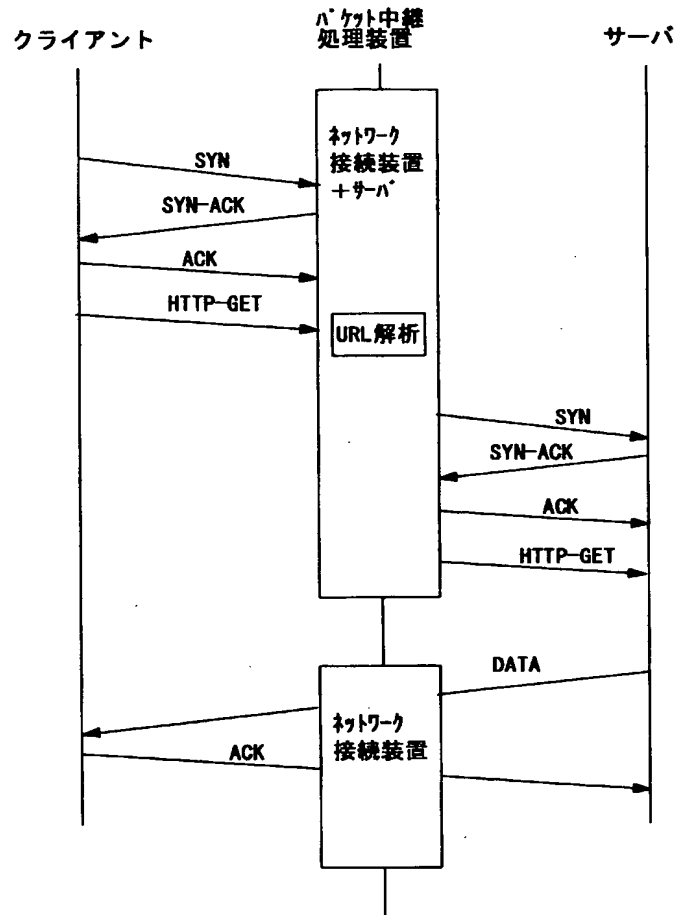
【図 22】

URLフィルタリングの動作を説明する図



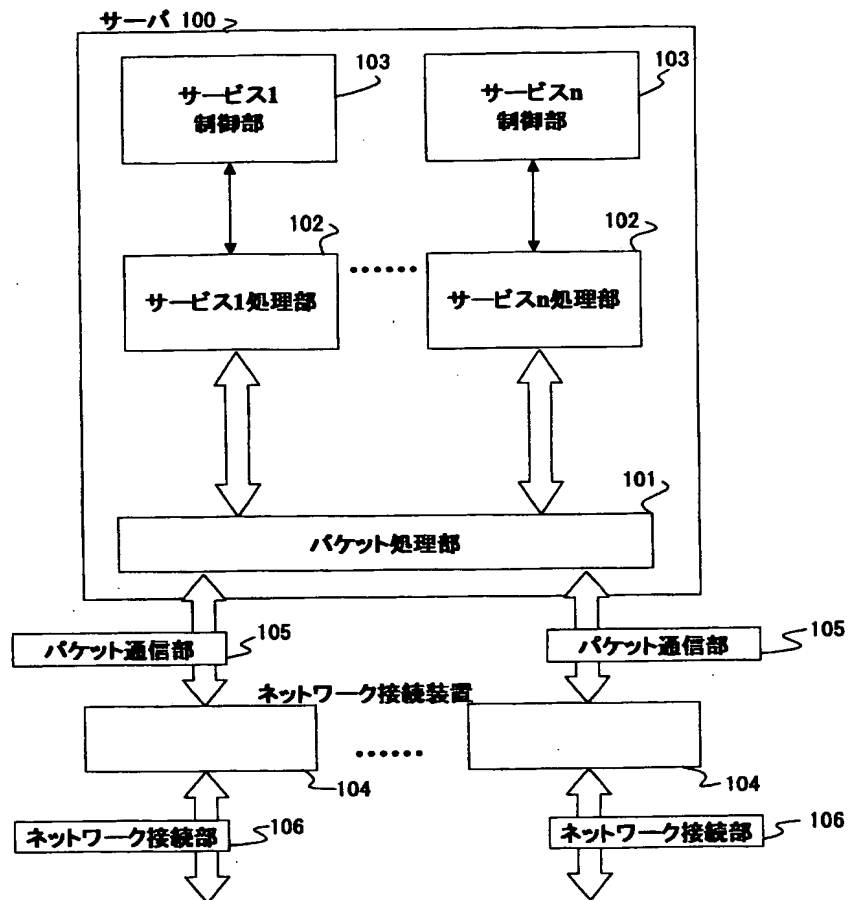
【図 2 3】

URL 負荷分散の動作を説明する図



【図 2 4】

従来のパケット中継処理装置の構成を示す図



【書類名】 要約書

【要約】

【課題】 多くのネットワークサービスで使用している共通処理を、ネットワーク接続装置に配置することにより、サーバのサービス処理を高速化すること。

【解決手段】 従来サーバ上に配置していたパケット処理部とセッション管理部をネットワーク接続装置 2 上に配置し、ネットワーク接続装置 2 上でセッション管理に基づくパケット中継処理を行う。また、ネットワーク装置 2 上に、処理振分部 2 c とサービス処理部 2 d を設け、サーバ 1 により設定されるポリシーに従って、処理振分部 2 c によりサービス処理部 2 d へのセッション管理に基づく振り分けを行う。さらに、条件に応じてサーバ 1 でセッション管理を行ったり、サーバにもサービス処理を行わせるようにしたり、サーバでパケットを解析してサービス内容を設定し、ネットワーク接続装置が、以後同じセッションに対して上記サービス内容に基づき中継処理を行うようにすることもできる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.